Patent Application of

Cynthia Gayle Eaker

for

SYSTEM AND METHOD FOR SECURE COMMUNICATION AND STORAGE OF INFORMATION

Background-Field of Invention

This invention relates to a system and method for secure communication and storage of information, specifically to an improved system and method that is ultra-secure and easy to use.

Background-Description of Prior Art

Encryption has been used to communicate privately for hundreds of years. The encryption systems and methods that now do so are numerous. But there is only one method known to be perfect in that it cannot be broken if used properly. The One Time Pad by Vernam in July 1919, patent number 1310719, is perfect in its ability to securely encrypt communication but to the same degree it is also impractical. This is because it requires the sender and receiver to have identical sets of random key pads that are as long and numerous as the messages being sent. The number of pads needed for sustained communications and the problem of securely distributing those pads is considerable. The perfect system is perfectly impractical.

Objects and Advantages

My above patent uses a practically endless number of unique digit sequences that are generated from a large fixed number of digits determined by a key. This results in a practical, ultra-secure, encryption system. It generates unpredictable digit sequences using a unique property of prime numbers. If a prime number of random digits are arranged in a ring the number of unique, unpredictable, digit sequences that can be made from it approaches that prime number squared. Each unique digit sequence made has the length of that prime number. The number of unique digit sequences is further increased by effective transposition of the digits and or summing multiple sequences together without carries.

In my system and method a multitude of unique digit sequences created using this method are used to change plaintext into ciphertext. The ciphertext is also well shuffled in over 10^150 ways using non-repeating digit sequences determined by the key and system and method used. The resulting coded messages consist of an unbroken string of 100 possible ciphertext characters that appear random in distribution until decoding shows that they are not.

Messages may be any information that can be digitized and transmitted by many means including, but not limited to, light signals, electromagnetic signals, audio signals, telephony networks, visual images, wired and wireless cable, satellite transmission, cellular phone signals, or computer networks. Accordingly, several objects and advantages of the present invention are:

(a) to provide an encryption system that forces codebreakers to resort to brute force attacks on the key used to code messages even though its length approaches 10^8,000 factorial.

(b) to provide elegant coded messages made up of an unbroken string of 100 unique coded characters that have no more than 5,010 ciphertext characters for every 5,000 characters of plaintext.

(c) to provide a coded message that will sometimes have fewer coded characters than the uncoded ones it came from by coding plaintext prior to encryption.

(d) To provide an ultra-secure encryption system and method that is easy to use.

(e) To provide an encryption method that can be set to automatically code and decode information to and from one or more senders with one or more keys.

(f) To provide a symmetric or asymmetric encryption system.

(g) to provide an encryption system and method that will be backward compatible and grow stronger as future versions increase the number of system and methods available to code messages with the system and method used to code messages always being indeterminable from examination of ciphertext.

(h) to provide an encryption system and method that will be easy to modify when the source code is made public allowing users to easily make their own unique mutation that is ultra-secure.

(i) to provide an encryption method that intersperses vital decoding information into the ciphertext.

(j) to provide an encryption method that uses numerous system and methods to code messages and intersperses the system and method information used in coding into the ciphertext.

(k) to provide an encryption system that thoroughly shuffles ciphertext characters after first breaking them into one or more components resulting in a very fine and complex rearrangement.

(l) to provide an encryption system that provides users computer-end security by intentionally corrupting, shuffling, and or removing vital digit arrangements used to code and decode.

(m) to provide an asymmetric encryption system that makes it statistically impossible to use identical digit sequences in the transformation phase of coding messages for up to 100 years.

(n) to provide an encryption system employing a large number of unique, unpredictable, digit sequences derived from skipping through a large prime number of digits in a ring at different starting points with skip sizes that vary which are then used to convert plaintext to ciphertext.

(o) to provide an encryption system that automatically corrects some of the negative effects of poor key choices and allows users to choose short or long keys.

(p) to provide an encryption system that has an easy to use parallel key making procedure resulting in a private key made publicly.

(q) to provide an encryption system that converts a key into unique digit sequences and a unique prime string of digits to code information.

(r) to provide an encryption system that can be used to easily generate random digit sequences.

Further objects and advantages of my invention will become apparent from a consideration of the ensuing explanation and detailed description.

Summary, Ramifications, and Scope

Accordingly, the reader will see that the encryption system and method of this invention can be used to easily code and decode information for secure storage and or transmission to self, individuals, or groups whether the information is in the form of text, audio, or images using ultra-secure encryption.

Cryptanalysts will find no shortcut to decoding ciphertext without knowing the key since frequency analysis on coded messages will yield no helpful clues. Frequency analysis will also become increasingly difficult since the system and method used to code any message is indeterminable and more systems and methods will be released over time. A brute force attack to determine the key will be necessary but equally

futile. This is because the key size may easily approach 10^8,000 factorial which is far larger than that thought necessary to provide security for hundreds, if not thousands, of years.

Users of the encryption system and method will appreciate that it is unbreakable for all practical purposes and that they have the flexibility of being able to choose short or long keys from plaintext or ciphertext that can themselves be coded for end security. They will also appreciate the ability to easily create a secure private key through an exchange of information on transmission lines known to be insecure.

Readers will appreciate the value of communications being automatically coded and decoded once a key is made. Recognizing that encrypted communications should be the norm just as it is the norm for private messages to be sent in sealed envelopes instead of being sent written on postcards.